



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 10/769,038 | 01/30/2004 | Daniel M. Bodorin | MSFT122168 | 7942 |
| 26389 | 7590 | 07/24/2008 | EXAMINER | |
| CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC 1420 FIFTH AVENUE SUITE 2800 SEATTLE, WA 98101-2347 | | | LASHLEY, LAUREL L | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2132 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 07/24/2008 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

| | | | |
|------------------------------|------------------------|---------------------|--|
| Office Action Summary | Application No. | Applicant(s) | |
| | 10/769,038 | BODORIN ET AL. | |
| | Examiner | Art Unit | |
| | LAUREL LASHLEY | 2132 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 14 April 2008.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-16 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ . | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/14/2008 has been entered. Claims 1 -16 are pending.

Response to Arguments

2. Applicant's arguments filed 04/14/2008 have been fully considered but they are not persuasive. As it relates to White, it is Applicant's assertion that White does not disclose recording some of the behaviors during execution of the code module and then comparing the recorded behaviors against recorded behaviors of known malware to identify/determine the code module as malware. The Examiner respectfully disagrees. White discloses that samples of virus activity are taken and further analyzed at the virus analysis center. For this to take place, White further discloses that samples of virus activity are created by replicating the virus by running in an emulated environment. It is after enough activity can be gleaned from replication that analysis can take place (see page 2, paragraph 2, 4 and 5 and Figure 6). Furthermore White discloses that virus samples are stored (see page 15, paragraph 4 and page 22, paragraph 7) and a comparison is made between the archived samples and the virus definition to determine exact matches (see page 23, paragraph 1). Only upon exact matches of behavior, which White notes as full verification, are any further actions taken.

Applicant also contends that White discloses matching checksums which is not the same as comparing the behavior signature of the sample to the known malware behavior signatures in

the malware behavior signature store to determine whether the exhibited execution behaviors of the sample match the exhibited execution behaviors of a known malware. The Examiner agrees with Applicant's analysis but would further like to clarify that in White, checksums are used to check or determine if a sample file is "infected" and if so, it is subjected to further analysis by the analysis center utilizing virus definitions (which are well known in the art to utilize virus signatures (i.e. virus pattern, behavior, fingerprint, etc.)) to specifically identify the type of virus (see pages 14-15). Therefore, it is through the analysis (i.e. comparison since "match" needs to be found) of virus signatures (virus definitions) that virus are identified.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless – (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-4 are rejected under 35 USC 102(b) as anticipated by White et al. ("Anatomy of a Commercial-Grade Immune System", <http://citeseer.ist.psu.edu/white99anatomy.html>, 1999), hereafter "White".
4. With regard to claims 1 and 2, White discloses a malware detection system and means for determining whether a code module is malware according to the code module's exhibited behaviors (Fig. 3, page 14), the system comprising:

at least one dynamic behavior evaluation module (Fig. 6, page 20, Analysis Center reads on dynamic behavior evaluation module), wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type (Section "Creation of the replication environment", Page 20: paragraph 1: lines 1-5), and wherein

each dynamic behavior evaluation module records some execution behaviors of the code module as it is executed, wherein the execution behaviors of the code module are recorded into a behavior signature corresponding to the code module: (Fig. 6, page 20: item "archive" and Section "Analysis", page 21: paragraph 1: lines 5-6, extract good signature and stores in the archive for developing virus definition reads on each dynamic behavior evaluation module records some behaviors which may be exhibited by the code module as it is executed into a behavior signature);

a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type (Fig. 3: page 20: item "workflow supervisor" and Section "Macro Viruses": page 25: paragraph 1: lines 5-7, supervisor accept suspected virus sample and feed into different virtual environment for each format and language of Macro Virus reads on a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type);

a malware behavior signature store storing at least one known malware behavior signature of a known malware (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file reads on malware behavior signature store storing at least one known malware behavior signature); and

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors

of a known malware (Section "An active network to Handle Epidemics and Floods – Overview", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware).

5. With regard to claim 3, White discloses a method for determining whether a code module is malware according to the code module's exhibited behaviors (Fig. 3, page 14), the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module (Fig. 3: page 20: item "workflow supervisor", page 19: paragraph 1 and 2, and Section "Macro Viruses", page 25: paragraph 1: lines 5-7, supervisor selects sample and dispatch to the particular system as described in Section "Marco viruses" reads on selecting a dynamic behavior evaluation module according to the executable type of the code module);

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed (Section "Creation of the replication environment", Page 20: paragraph 1 and 2);

recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module during execution of the code module (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file

reads on recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module);

comparing the recorded execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware execution behaviors (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors); and

according to the results of the previous comparison, determining whether the code module is malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 3: lines 1-6, gateway scans the sample to see if it can handle the sample by itself reads on according to the results of the previous comparison, determining whether the code module is malware).

6. With regard to claim 4, White discloses a computer-readable medium bearing computer-executable instructions which, when executed, carry out a method for determining whether an executable code module is malware according to the code module's exhibited behaviors (Fig. 5: page 18) , the method comprising selecting a dynamic behavior evaluation module according to the executable type of the code module (Fig. 3: page 20: item "workflow supervisor", page 19: paragraph 1 and 2, and Section "Macro Viruses", page 25: paragraph 1: lines 5-7, supervisor selects sample and dispatch to the particular system as described in Section "Marco viruses" reads on selecting a dynamic behavior evaluation module according to the executable type of the code module);

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed (Section "Creation of the replication environment", Page 20: paragraph 1 and 2);

recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file reads on recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module);

comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors (Section "An active network to Handle Epidemics and Floods – Overview", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors); and

according to the results of the previous comparison, determining whether the code module is malware (Section "An active network to Handle Epidemics and Floods – Overview", pages 13-15: paragraph 3: lines 1-6, gateway scans the sample to see if it can handle the sample by itself reads on according to the results of the previous comparison, determining whether the code module is malware).

For claim 5 and similar claims 8, 11 and 14, White discloses wherein recording some execution behaviors of the code module as it is executed comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record (page 21, paragraph 5: virus definition...set of source files...virus analysis).

For claim 6 and similar claims 9, 12, and 15, White discloses wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed. (Fig. 3: page 20: item "workflow supervisor" and Section "Macro Viruses": page 25: paragraph 1: lines 5-7, supervisor accept suspected virus sample and feed into different virtual environment for each format and language of Macro Virus reads on a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type; page 19, paragraph 3 and paragraph 5: virus definition version...superset of previous definition...; page 20, paragraph 1 "classification"...determine type...)

For claim 7 and similar claims 10, 13 and 16, White discloses wherein the predefined set of execution behaviors to record corresponds to a set of system calls (page 20, paragraph 1 "classification".

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Schultz et al. in US Patent Application Publication No. 20030065926 discloses a system and method for detection of new malicious executables.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAUREL LASHLEY whose telephone number is (571)272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Laurel Lashley/
Examiner, Art Unit 2132

07/18/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132